UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,753	11/26/2003	Choon B. Shim	1370.215US1	3938

21186 7590 09/03/2009

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
09/03/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@slwip.com
request@slwip.com

Office Action Summary	Application No.	Applicant(s)	
	10/721,753	SHIM ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 May 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed May 15, 2009. Claims 1, 16 and 21 have been amended. Claims 1-22 are pending and have been considered below.

Response to Arguments

2. Applicant's arguments with respect to claims 1-22 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

3. The rejection to claims 9-15 has been withdrawn, however claims 16-20 are still rejected, the claims recite the limitations of proxy server, the firewall, the control unit, or the first console can be either software, hardware, or a combination. They are directed to an apparatus, but there is no apparatus, just code. Applicant's argument regarding the 101 rejection of claims 16-20 is not persuasive, Therefore the 101 rejection has been maintained. The rejection regarding claims 21 and 22 has been withdrawn in light of the amendment.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 3, 6, 7, 16 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sit et al (US 6,349,336) in view of Grantges, Jr herein after Grantges (US 6,324,648).

Regarding claim 1, Sit et al teaches

configuring a first control unit, inside a first firewall , the first control unit separate from the first firewall and used to control the network (column 7, lines 15-40: fig. 5, 306);

configuring a proxy server outside the first firewall (Fig. 5, 312); and

Sit et al does not explicitly disclose establishing a session between the first control unit and the proxy server, wherein establishing the session is executed using an access key, nor a step of establishing a connection between the proxy server and a console, to permit remote user management of the network by communication between the first control unit and the console via the proxy server. However, Grantges, discloses a secure gateway , which further discloses

establishing a session between the first control unit and the proxy server, wherein establishing the session is executed using an access key (*column 6, lines 37-67*).

establishing a connection between the proxy server and a console, to permit remote user management of the network by communication between the first control unit and the console via the proxy server(column 14, lines 25-55).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to establish a session using an access key and to permit remote user management of network. The motivation of doing so would have been provide access from a client computer over an insecure public network to one of the plurality destination servers on a secure private network (see Grantges, Column 1, lines 10-15).

Regarding claim 16, Sit et al teaches

a first console residing within an unprotected public network and configured to generate at least one console request message, the console request message including at least one of a request for network management data, a request for Internet Protocol (IP)-Private Branch Exchange (PBX), or a request for status information (column 7, lines 15-40: fig. 5);

a proxy server coupled to the first console, the proxy server configured to pool the at least one request, and to provide access from at least one console to the first control unit and to aggregate and store performance data provided by the first control unit, the proxy server being implemented within a De-Militarized Zone (DMZ) between a protected network and the unprotected public network (fig.2, 255);

a first firewall coupled to the proxy server ((column 7, lines 15-40: fig. 5, 305);and

a first control unit residing within the protected network and coupled to the first firewall, the first control unit configured to receive the at least one request from the proxy server, the first control unit further configured to output at least one response corresponding to the at least one request to the proxy server, the proxy server configured to output the at least one response to the first console (column 7, lines 15-40: fig. 5, 306).

Sit et al does not explicitly disclose that the proxy server being implemented within a De-Militarized Zone. However, Grantges, discloses a secure gateway , which further discloses the proxy server being implemented within a De-Militarized Zone (column 4, lines 1-25; Fig. 1).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made such as to being implemented a proxy server within a De-Militarized Zone. The motivation of doing so would have been provide access from a client computer over

an insecure public network to one of the plurality destination servers on a secure private network (see Grantges, Column 1, lines 10-15).

Regarding claim 3, Sit et al and Grantges teach the method as in claim 1, and while neither of them expressly disclose, however, Examiner takes Official Notice that configuring the first control unit includes: receiving the proxy server identification information; generating an access key in the first control unit; and sending the access key and first control unit identification information to the proxy server. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to configure a first unit for security purposes as claimed since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 6, Sit et al and Grantges teach the method as in claim 1, and Grantges teaches wherein configuring the proxy server includes: receiving the first control unit identification information(column 6, lines3-13); storing the first control unit identification information in the proxy server(column 6, lines 10-35); adding the first control unit as a first remote device; and exchanging a validation message between the first control unit and the proxy server (column 6, lines 3-30).

Regarding claim 7, Sit et al and Grantges teach the method as in claim 1, while either of them expressly disclose, however, Examiner takes Official Notice that wherein establishing a session between the first control unit and the proxy server includes coupling through a second firewall, the proxy server being inside the second firewall. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to configure a first unit for security purposes as claimed since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 20, Sit et al and Grantges teach the system as in claim 16, and Grantges teaches wherein the proxy server includes processor- executable code, the code performing the steps of: receiving a client request from the first console(Fig.2); writing the at least one request(column 4, fines 1-20, column 5, line 40 to column 6, line 67; reading the at least one request; sending the at least one request to the first control unit (column 4, lines 1-20, column 5, fine 40 to column 6, line 67); sending the at least one request to the first control unit column 4, lines 1- 20, column 5, line 40 to column 6, line 67); receiving the at least one response; and outputting the at least one response to the first console (column 4, lines 1- 20, column 5, line 40 to column 6, line 67)).

6. Claims 9, 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sit et al (US 6,349,336) in view of Grantges, Jr herein after Grantges (US 6,324,648) in further view of Schweitzer (US 2002/0038364).

Regarding claim 9, Sit et al teaches

a first enterprise network (column 7, lines 15-40: fig. 5, 302);

a first control unit coupled to the first enterprise network (column 7, lines 15-40: fig. 5, 306);

a first firewall coupled to the first control unit, the first firewall and first control unit being separate (column 7, lines 15-40: fig. 5, 305);

a public network (column 7, lines 15-40: fig. 5, 301);and

a proxy server located outside the first fire wall and implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network, the first control unit

being configured with proxy server information, the proxy server being configured with first control unit information, the first control unit being further configured to send a first access key to the proxy server, the first control unit and the proxy server configured to establish a communication session based on the first access key, the proxy server to aggregate and store performance data provided by the first control unit.

Sit et al does not explicitly disclose a proxy server located outside the first fire wall and implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network, the first control unit being configured with proxy server information, the proxy server being configured with first control unit information, the first control unit being further configured to send a first access key to the proxy server, the first control unit and the proxy server configured to establish a communication session based on the first access key, the proxy server to aggregate and store performance data provided by the first control . However, However, Grantges, discloses a secure gateway a proxy server located outside the first fire wall and implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network(column 5, lines 58-68), the first control unit being configured with proxy server information, the proxy server being configured with first control unit information, the first control unit being further configured to send a first access key to the proxy server, the first control unit and the proxy server configured to establish a communication session based on the first access key (*column 6, lines 37-67; column 8, lines40-55*).while neither of them disclose a step of aggregating and storing performance data provided by the first control unit. Schweitzer discloses a system for handling network accounting, which further discloses the proxy server to aggregate and store performance data provided by the first control unit(paragraph [0034]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to establish a session using an access key and to permit remote user management of network. The motivation of doing so would have been provide access from a client computer over an insecure public network to one of the plurality destination servers on a secure private network (see Grantges, Column 1, lines 10-15). The motivation to modify the combined teaching of Sit et al and Grantges such as to sore and aggregate performance would have been to effect improvements in system speed and performance(see Schweitzer paragraph [0007]).

Regarding claim 12, Sit et al teaches

a first enterprise network (column 7, lines 15-40: fig. 5, 302);

a first control unit coupled to the first enterprise network ((column 7, lines 15-40: fig. 5, 306);

a first firewall coupled to the first control unit, the first firewall and first control unit being separate (column 7, lines 15-40: fig. 5, 305);

a public network ((column 7, lines 15-40: fig. 5, 301); and

a proxy server, to aggregate and store performance data provided by the first control unit, that includes at least one of a client request handler, a shared request object pool, or a server request handler, the proxy server being implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network (column 7, lines 15-40: fig. 5, 305).

Sit et al does not explicitly disclose a proxy server, to aggregate and store performance data provided by the first control unit, that includes at least one of a client request handler, a shared request object pool, or a server request handler, the proxy server being implemented

within a De-Militarized Zone (DMZ) between the first enterprise network and the public network (fig.2, 255). However, Grantges, discloses a secure gateway, which further discloses a proxy server, to aggregate and store performance data provided by the first control unit, that includes at least one of a client request handler, a shared request object pool, or a server request handler, the proxy server being implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network (column 5, lines58-67), while neither of them disclose a step of aggregating and storing performance data provided by the first control unit. Schweitzer discloses a system for handling network accounting, which further discloses the proxy server to aggregate and store performance data provided by the first control unit (*paragraph [0034]).*

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to establish a session using an access key and to permit remote user management of network. The motivation of doing so would have been provide access from a client computer over an insecure public network to one of the plurality destination servers on a secure private network (see Grantges, Column 1, lines 10-15). The motivation to modify the combined teaching of Sit et al and Grantges such as to sore and aggregate performance would have been to effect improvements in system speed and performance(see Schweitzer paragraph [0007]).

Regarding claim 13, Sit et al and Grantges teach the system as in claim 12, and Grantges teaches wherein the proxy server is configured to receive first control unit identification information, store the first control unit identification information in the proxy server, add the first control unit as a first remote device, and exchange a validation message between the first control unit and the proxy server (column 6, lines 12-35).

7. Claims 2, 4, 5, 8, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sit et al (US 6,349,336) in view of Grantges, Jr herein after Grantges (US 6,324,648) in further view of Xu et al (US 7,257,837).

Regarding claim 2, Sit et al and Grantges teach the method as in claim 1, while neither of them explicitly configuring a second control unit inside a second firewall, the proxy server being outside the second firewall. However, Xu et al discloses a firewall penetration system for real time media communications, which further discloses that the method further comprising configuring a second control unit inside a second firewall, the proxy server being outside the second firewall (*Fig. 1*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges, Jr. et al such as to include a second firewall. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

Regarding claim 4, ,Sit et al and Grantges teach the method as in claim 3 and while neither of them explicitly disclose wherein receiving the proxy server identification information includes receiving a proxy server host name, a proxy server IP address, and a proxy server port number. Xu et al further discloses wherein receiving the proxy server information includes a proxy server host name, a proxy server IP address, and a proxy server port number (column 2, lines 45-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges, such as to include a proxy server host name, a proxy server IP address, and a proxy server port number. One would have been

motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

Regarding claim 5, Sit et al and Grantges teach the method as in claim 3, while neither of them explicitly discloses wherein receiving the proxy server identification information includes inquiring the proxy server from the first control unit to obtain the proxy server IP address. Xu et al f discloses wherein receiving the proxy server identification information includes inquiring the proxy server from the first control unit to obtain the proxy server IP address (column 4, lines24-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges, Jr. et al such as to include a second firewall. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

Regarding claim 8, Sit et al and Grantges teach the method as in claim 7, while neither of them explicitly discloses connecting between the proxy server and a console, the console being inside the second firewall, the connecting using an IP address facing inside the second firewall. Xu et al further discloses connecting between the proxy server and a console, the console being inside the second firewall, the connecting using an IP address facing inside the second firewall (column 4, lines 24-67; Fig. 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges such as to include a second firewall. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

Regarding claim 17, Sit et al and Grantges teach the system as in claim 16, while neither of them explicitly disclose but does not explicitly discloses a second console coupled to the proxy server, the second console configured to generate at least one other request, the proxy server configured to pool the at least one other request. However, Xu et al discloses a firewall penetration system for real time media communications, which further discloses a second console coupled to the proxy server, the second console configured to generate at least one other request, the proxy server configured to pool the at least one other request(Fig. 1). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges such as to include a second console. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10) teaches a second console coupled to the proxy server, the second console configured to generate at least one other request, the proxy server configured to pool the at least one other request (fig.2, 210).

Regarding claim 18, Sit et al and Grantges teach the system as in claims 16, and Xu et al further disclose that a second firewall coupled to the public network; a second control unit coupled to the second firewall(Fig.1); and

a second enterprise network coupled to the second control firewall, the second control unit being configured with proxy server information, the proxy server being configured with second control unit information, the second control unit being further configured to send a second access key to the proxy server, the second control unit and the proxy server configured to establish a communication session based on the second access key(column 4, line 16 to column 5, line45; Fig.1). Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify the teaching of Grant,qes such as to include and configure a second firewall. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

8. Claims 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sit et al (US 6,349,336) in view of Grantges, Jr herein after Grantges (US 6,324,648) in further view of Devine (US 6,968,571).

Regarding claim 19, Sit et al and Grantges teach the system as in claim 16, while neither of them explicitly discloses wherein the proxy server includes: a client request, a shared request object pool, a server request handler, and a shared request object pool. However Devine et al discloses a secure customer interface for web based data management, which further discloses

A client request handler for receiving a client request from the first console (*column 18, lines 59-67*);

A shared request object pool coupled to the client request handler, the shared request object pool configured to store the at least one request (*column 21, lines 1-15*); and

A server request handler coupled to the shared request object pool*(column 21, lines 13-35)*, the server request handler configured to read the at least one request from the shared request object pool, the server request handler configured to send the at least one request to the first control unit, the server request handler configured to receive the at

least one response, the server request handler configured to output the at least one response to the first console(*column 18, line 59 to column 19 , line 20*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges, Jr. et al such as to include in the proxy server includes: a client request, a shared request object pool, a server request handler, and a shared request object pool. One would have been motivated to do so in order to provide a security methodology for connecting users to an enterprise network or extranet over the public Internet as taught by Devine et al (column 1, lines 20-25).

9. Claims 10, 11, 14, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sit et al (US 6,349,336) in view of Grantges, Jr herein after Grantges (US 6,324,648) in further view of Schweitzer (US 2002/0038364) and Xu et al (US 7,257,837).

Regarding claim 10, Sit et al , Grantges and Schweitzer teach the method as in claim 9, and while neither of them explicitly disclose wherein receiving the proxy server identification information includes receiving a proxy server host name, a proxy server IP address, and a proxy server port number. Xu et al further discloses wherein receiving the proxy server information includes a proxy server host name, a proxy server IP address, and a proxy server port number (column 2, lines 45-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges, such as to include a proxy server host name, a proxy server IP address, and a proxy server port number. One would

have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

Regarding claims 11 and 14, Sit et al , Grantges and Schweitzer teach the system as in claims 9 and 13, and Xu et al further disclose that a second firewall coupled to the public network; a second control unit coupled to the second firewall(Fig.1); and

a second enterprise network coupled to the second control firewall, the second control unit being configured with proxy server information, the proxy server being configured with second control unit information, the second control unit being further configured to send a second access key to the proxy server, the second control unit and the proxy server configured to establish a communication session based on the second access key(column 4, line 16 to column 5, line45; Fig.1). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Sit et al , Grantges and Schweitzer such as to include and configure a second firewall. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10)

Regarding claim 15, Sit et al , Grantges , Schweitzer and Xu et al teach the system as in claim 14, and Xu et al further discloses wherein the proxy server is configured to receive second control unit identification information, store the second control unit identification information in the proxy server, add the second control unit as a second remote device, and exchange a validation message between the second control unit and the proxy server (*column 10 line 11column 11, line 50*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Sit et al , Grantges and Schweitzer, Jr.

et al such as to include second firewall, a second control unit and a second enterprise network. One would have been motivated to do so in order to enable authentication between entities in communication.

10. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Devine(US 6,968,571) in view of Smith (6,341,311).

Regarding claim 21, Devine teaches

At a proxy server receiving a console request message from a console, the console request message including at least one of a request for network management data, a request for Internet Protocol (IP)-Private Branch Exchange (PBX), or a request for status information (column 8, lines 15-60; column 9, lines 15-35; Fig. 9);

Using a processor, automatically creating a request object; adding the request object to a pool; and notifying a control unit of the request object, the control unit being inside of a firewall (column 14, lines 10-30).

Devine does not explicitly disclose the creation of a request object and addition of the request object to a pool. However, Smith et al discloses a method of detecting data object request, which further disclose the creation of a request object and addition of the request object to a pool (column 21, lines 15-30) .Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made create and addition of request object to a pool of object. The motivation of doing so would have been to utilize deterministic hashing algorithms to allow consistent and predictable identification of a proxy server to be assigned or have residing thereon a particular URL data object (see Smith et al, column 4, lines 25-55)

Regarding claim 22, Devine and Smith et al teach the method as in claim 1, and Devine teaches establishing a data connection with the control unit; receiving a request from the control unit for the request object; sending the request object to the control unit; receiving a response from the control unit based on the request object; and sending the response to the console (column 18, lines59-67; column 21, lines 1-15).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

Friday August 28, 2009.

/F. T./

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436